CEA ACTION PROPOSAL

Per California Code of Regulations, title 2, section 548.5, the following information will be posted to CalHR's Career Executive Assignment Action Proposals website for 30 calendar days when departments propose new CEA concepts or major revisions to existing CEA concepts. Presence of the department-submitted CEA Action Proposal information on CalHR's website does not indicate CalHR support for the proposal.

A. GENERAL INFORMATION

1. Date: March 8, 2023

2. Department: Department of Justice

3. Organizational Placement (Division/Branch/Office Name)

Directorate Division, Office of the General Counsel, Information Security Office

4. CEA Position Title

Chief Information Security Officer

5. Summary of proposed position description and how it relates to the program's mission or purpose. (*2-3 sentences)*

The Chief Information Security Officer (CISO), under the direction of the General Counsel, provides direction and policy guidance to the Information Security Office and the entire department as a whole on information security and privacy across all of the DOJ's platforms, databases, applications, and enterprises. This position has broad authority and management responsibility for protecting the privacy, confidentiality, integrity, and availability of the DOJ's information and services while ensuring compliance with state and federal information security policies, standards, and procedures.

6. Reports to: (*Class Title/Level*)

General Counsel, CEA C

7. Relationship with Department Director (*Select one)*

☐ Member of department's Executive Management Team, and has frequent contact with director on a wide range of department-wide issues.

☑ Not a member of department's Executive Management Team but has frequent contact with the Executive Management Team on policy issues.

(*Explain*): This position is responsible for policy and direction over information security. The incumbent will be required to report any major changes or concerns to the General Counsel, who is a member of the Executive Management Team.

8. Organizational Level *(Select one)*

☐ 1st ☐ 2nd ☑ 3rd ☐ 4th ☐ 5th (mega departments only - 17,001+ allocated positions)

B. SUMMARY OF REQUEST

9. What are the duties and responsibilities of the CEA position? Be specific and provide examples.

The CISO will direct the strategy, planning, development and enforcement of information security policies, standards, and procedures which protect the confidentiality, integrity, and availability of DOJ data and its IT systems and applications. This position will also facilitate governance of information security within the DOJ. The CISO will provide direction, policy advice, and training to the Office of Program Oversight and Accountability, Research Services, Cybersecurity Branch and the Security Risk Management Unit. These sections are tasked with protecting the security of tens of millions of records relating to the areas of criminal history, biometric data, DNA, firearms, litigation, legal services, and case management. The CISO is responsible for security policy maintenance and education, risk management, threat mitigation, vulnerability assessments, investigation of security and privacy incidents, security compliance assessments, security architecture planning, technology recovery planning, and maintenance and oversight of security agreements with external partners.

The CISO will routinely consult with the General Counsel on sensitive and time-critical policy issues to ensure compliance with policies, procedures, and processes that are consistent with the organization's goals, objectives, and federal and state laws. The CISO will also confer with DOJ's executive level management on the most complex IT security issues regarding DOJ's databases and applications. The incumbent may represent the General Counsel and the AG at meetings with federal, state and local law enforcement agencies, cybersecurity organizations, and the Legislature. The CISO is responsible for strategic planning and coordination with DOJ executive management and external stakeholders. The incumbent will monitor and make policy recommendations on the impacts of legislation and regulation related to the security and confidentiality of DOJ's IT infrastructure, represent the DOJ in coordinating information security issues and requirements with California state control agencies, federal agencies, other state and local agencies, and individuals, and keep abreast of DOJ security incidents. The incumbent will also be responsible for ensuring all information technology and security related audits are kept focused on scope, tracked, and submitted on time and provide guidance, evaluation, and advocacy on audit responses.

The CISO will also create and maintain policies to provide a comprehensive risk management and communication framework that includes risk appetite, risk calculation, risk assessment methodologies, risk acceptance criteria, and the identification of risk categories. These policies are needed to track cyber threat and fraud issues from identification through resolution, and to develop a strong IT security risk program to meet current and future IT security assessments and audit requirements. The CISO will take a leading role in overseeing cybersecurity enhancements, suspicious activity monitoring tools, and staff training to proactively address cybersecurity vulnerabilities, threats and security findings, implement technology to prevent security breaches, meet the increasing need in cyber risk management, and strengthen the DOJ's cybersecurity posture.

Additional duties include review and approval of security plans and procedures, technology recovery plans, formal submissions to state and federal entities, and policy exceptions. The CISO will help safeguard the integrity and security of the DOJ information assets, and ensure stringent laws related to cybersecurity are fairly and adequately enforced.

B. SUMMARY OF REQUEST (continued)

10. How critical is the program's mission or purpose to the department's mission as a whole? Include a description of the degree to which the program is critical to the department's mission.

- ☑ Program is directly related to department's primary mission and is critical to achieving the department's goals.
- ☐ Program is indirectly related to department's primary mission.
- ☐ Program plays a supporting role in achieving department's mission (i.e., budget, personnel, other admin functions).

Description: The primary mission of the department is to serve our state and work honorably every day to fulfill California's promise. The AG and our Department's employees provide leadership, information and education in partnership with state and local governments and the people of California to enforce and apply all our laws fairly and impartially, ensure justice, safety, and liberty for everyone, encourage economic prosperity, equal opportunity and tolerance, and safeguard California's human, natural, and financial resources for this and future generations.

The CISO will directly support the DOJ’s mission by establishing and developing policy, standards and procedures to protect the department’s platforms, databases, applications, and enterprises. The CISO will direct security efforts to prevent, restrict and address sources of disruption to data stored within DOJ databases and applications. The incumbent will perform a leading role in overseeing cybersecurity enhancements, suspicious activity monitoring tools, and staff training to proactively address cybersecurity vulnerabilities, threats and security findings, implement technology to prevent security breaches, meet the increasing need in cyber risk management, and strengthen the DOJ’s cybersecurity posture.

B. SUMMARY OF REQUEST (continued)

11. Describe what has changed that makes this request necessary. Explain how the change justifies the current request. Be specific and provide examples.

California regulations and statues places a responsibility on state agencies as a whole, and the DOJ specifically, to not only maintain varied network, databases, and applications, but to protect the information contained therein. According to the State Administrative Manual section 5305, each state entity is responsible for establishing an information security program to effectively manage risk, provide for the protection of information assets and prevent illegal activity, fraud, waste, and abuse in the use of information assets. While the DOJ has this program in place, the threat of security breaches has significantly increased over the years with increasingly complex technology platforms.

The cyber threat landscape faced by California is very complex. Cyber-attacks on government resources, including DOJ's California Law Enforcement Telecommunications System (CLETS), firearms systems, and other DOJ systems, are becoming more and more prevalent. On average, DOJ Internet facing systems are scanned over 20,000 times a day by attackers looking for vulnerabilities with the number trending up every month. In addition to projection outward with investigative services, DOJ must bolster its resources for protecting internal information as well.

Over the years, the DOJ has been impacted by legislative mandates and internal initiatives which, expressly and/or implicitly, have expanded the size, reach, and responsibilities. For example, the California Justice Information Services (CJIS) Division houses and is tasked with protecting the security of tens of millions of records relating to the areas of criminal history, healthcare, biometric data, DNA, firearms, litigation, legal services, and case management, among others. Should any of the security of any of these records be compromised, the resulting impact to Californians could be devastating. The department also maintains the California Law Enforcement Telecommunications System (CLETS), which processes approximately one billion law enforcement transactions each year. All of the records maintained within CLETS are highly sensitive in nature and must be handled with the highest degree of skill and discretion.

In addition to its defensive cybersecurity responsibilities, DOJ has numerous statutory mandates requiring or allowing it to disclose data to law enforcement agencies, researchers, and the public. The volume of these disclosures has increased over the years as the Legislature has required that DOJ disclose information from an increasingly diverse set of programs, including electronic search warrants, police stops, and firearms-related information, among other program areas. A CISO is needed to ensure consistency in DOJ's disclosure policies. A CISO is also needed to coordinate and balance DOJ's extensive maintenance and security obligations with DOJ's disclosure responsibilities.

C. ROLE IN POLICY INFLUENCE

12. Provide 3-5 specific examples of policy areas over which the CEA position will be the principle policy maker. Each example should cite a policy that would have an identifiable impact. Include a description of the statewide impact of the assigned program.

The CISO will direct the strategy, planning, development and enforcement of information security policies, standards, and procedures which protect the confidentiality, integrity, appropriate use, and availability of DOJ information assets. The CISO will develop and maintain DOJ's security policies described in the State Administrative Manual (SAM), Section 5300 to frame, assess, respond, and monitor risk, which applies to all electronic data created, stored, processed or transmitted and computing environments, processes, systems, and applications.

Specific examples of policy areas for which the CEA will be the principle policy maker include, but are not limited to, the following:

California Government Code (GC) 15150-15167 state that the DOJ shall maintain a statewide telecommunications system for the use of law enforcement agencies. CLETS is an efficient law enforcement communications network available to all public agencies of law enforcement within the state. The CLETS provides all law enforcement and criminal justice user agencies with the capability of obtaining information directly from federal and state computerized information files. This position will be responsible for developing and implementing security policies over CLETS to ensure the transfer and storage of information within the system is secure.

Executive Order B-34-15 – Increase California’s preparedness to respond to cyber-attacks - All state departments and agencies must ensure compliance with existing information security and privacy policies, promote awareness of information security standards with their workforce, and assist the California Governor’s Office of Emergency Services and the California Cybersecurity Integration Center in executing this order. Given the threat of increasingly sophisticated cyber-attacks aimed at breaching and damaging computer networks and infrastructure in California, the CISO will work in coordination with the Cybersecurity branch and in consultation with the General Counsel, to ensure the organization meets all information security requirements.

SAM Section 5305.6 - Risk Management - Each state entity shall create a state entity-wide information security, privacy and risk management strategy which includes a clear expression of risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization. The CISO will implement policies for risk assessments and processes to manage vulnerabilities within the DOJ's information processing infrastructure.

SAM Section 5340 - Information Security Incident Management - Each state entity must promptly investigate incidents involving loss, theft, damage, and misuse of information assets, or improper dissemination of information. All state entities are required to report information security incidents consistent with the security reporting requirements stated in this policy and manage information security incidents to determine the cause, scope, and impact of incidents. Through review and implementation of policies and guidelines, the CISO will manage threats and incidents impacting DOJ's information resources and assets.

SAM Section 5325.1 - Technology Recovery Plan (TRP) - Each state entity shall develop a TRP in support of the state entity’s Continuity Plan and the business need to protect critical information assets to ensure their availability following an interruption or disaster. Each state entity must keep its TRP up-to-date. This position will oversee DOJ’s operational and disaster recovery plans for all DOJ information assets, including CLETS. This is especially important as the information stored within CLETS should be available 24x7 to all California law enforcement agencies.

C. ROLE IN POLICY INFLUENCE (continued)

13. What is the CEA position's scope and nature of decision-making authority?

The CISO will provide policy advice and guidance to the AG, the CDAG, General Counsel, and the CJIS Division Chief, as well as advise departmental senior management regarding the security of DOJ's IT infrastructure. This position will serve in a policy influencing role which will impact the department as a whole.

The CISO position has extensive decision making authority and provides vision and leadership for developing and supporting security initiatives. The incumbent directs the planning and implementation of enterprise IT systems against security breaches, vulnerability, and fraud, to prevent, restrict and address sources of disruption. The CISO will consult with the General Counsel on sensitive and time-critical IT security policy issues to ensure division compliance with policies, procedures, and processes that are consistent with the organization’s goals, objectives, and federal and state laws. The CISO will monitor and make policy recommendations on the impacts of legislation and regulation related to security of DOJ's IT infrastructure.

14. Will the CEA position be developing and implementing new policy, or interpreting and implementing existing policy? How?

The CISO will be responsible for developing new policies, evaluating existing policies and providing direction on the security of DOJ's IT infrastructure, which impacts DOJ employees, various law enforcement entities, the public, and other local, state and federal agencies. These entities depend on having secure criminal history information which is stored in databases maintained by the DOJ's IT bureaus. As new policy and/or legislative mandates are set, the CISO will be responsible for developing and implementing new IT security policies and procedures to ensure DOJ's IT infrastructure is secure and able to keep up with the ever changing and increasingly complex technological landscape. These policies and procedures will aim to prevent data breaches, phishing, malware, and develop robust safety protocols.